

## WEST Search History






DATE: Monday, June 27, 2005

<u>Hide?</u>	<u>Set Name</u>	<u>Query</u>	<u>Hit Count</u>
		<i>DB=USPT; PLUR=NO; OP=OR</i>	
<input type="checkbox"/>	L24	L23 and "personal information"	221
<input type="checkbox"/>	L23	L22 and grant\$	2650
<input type="checkbox"/>	L22	L21 and permission	7289
<input type="checkbox"/>	L21	user and information	247920
<input type="checkbox"/>	L20	L19 and user and information	7289
<input type="checkbox"/>	L19	permission	11846
<input type="checkbox"/>	L18	(235/382)[CCLS]	928
<input type="checkbox"/>	L17	(235/381)[CCLS]	748
<input type="checkbox"/>	L16	(235/380)[CCLS]	2518
<input type="checkbox"/>	L15	(705/44)[CCLS]	300
<input type="checkbox"/>	L14	(705/74)[CCLS]	53
<input type="checkbox"/>	L13	(705/59)[CCLS]	191
<input type="checkbox"/>	L12	(705/58)[CCLS]	129
<input type="checkbox"/>	L11	(705/57)[CCLS]	334
<input type="checkbox"/>	L10	(705/56)[CCLS]	97
<input type="checkbox"/>	L9	(705/55)[CCLS]	87
<input type="checkbox"/>	L8	(705/545)[CCLS]	0
<input type="checkbox"/>	L7	(705/54 ) [CCLS]	103
<input type="checkbox"/>	L6	(705/53 ) [CCLS]	95
<input type="checkbox"/>	L5	(705/52 ) [CCLS]	185
<input type="checkbox"/>	L4	(705/51 ) [CCLS]	426
<input type="checkbox"/>	L3	(705/5 ) [CCLS]	215
<input type="checkbox"/>	L2	(705/1 ) [CCLS]	876
<input type="checkbox"/>	L1	(705/1 ) ! [CCLS]	2

END OF SEARCH HISTORY



Top :

 **Dynamic Search:** ABI/INFORM®, Gale Group Computer Database(TM), Business & Industry(TM), Financial Times Fulltext, Business Wire (Mar 1999-present), The McGraw-Hill Companies Publications Online, Business Wire (1986-Feb 1999), Gale Group New Product Announcements/Plus®

Search History

save as alert

save strategy only

Select	Set	Searched for	In	Records
<input type="radio"/>	S4	Sort S3/1-500/PD,D	All subject words	500
<input type="radio"/>	S5	"PERSONAL INFORMATION"	All subject words	1
		Combined with set 4		
<input type="radio"/>	S6	Sort S5/1-500/PD,D	All subject words	1
<input type="radio"/>	S7	"PERSONAL INFORMATION"	All subject words	1
		Combined with set 4		
<input checked="" type="radio"/>	S8	Sort S7/1-500/PD,D	All subject words	1

[See all sets](#)

show picklist

Search Form

run saved strategy

Search for  In  
  
☒ Within selected search history set

clear

search >>

Database List

Database Name

♦ ABI/INFORM® (File 15)

♦ Gale Group Computer Database (TM) (File 275)

♦ Business & Industry(TM) (File 9)

♦ Financial Times Fulltext (File 476)

Database Name

♦ Business Wire (Mar 1999-present) (File 610)

♦ The McGraw-Hill Companies Publications Online (File 624)

♦ Business Wire (1986-Feb 1999) (File 810)

♦ Gale Group New Product Announcements/Plus® (File 621)

**DialogWeb**

Guided Search | new search | favorites | settings | order | cost | login | help

Dynamic Search: ABI/INFORM®, Gale Group Computer Database(TM), Business & Industry(TM), Financial Times Fulltext, Business Wire (Mar 1999-present), The McGraw-Hill Companies Publications Online, Business Wire (1986-Feb 1999), Gale Group New Product Announcements/Plus®

Records for: **"personal information"** [save as alert...](#) [save strategy only...](#)

Output: ☐ Format: **Full Record** Output as: **Browser** [display/send](#)

Modify: ☐ [refine search](#) [back to picklist](#)

[select](#) [print](#) [email](#) [print](#) [email](#)

**Records 1 of 1 In full Format**

 **Fulltext available through:** **USPTO Full Text Retrieval Options**

- ☐ 1. **6/9/1 (Item 1 from file: 15) DIALOG(R)File 15:ABI/Inform(R) (c) 2005 ProQuest Info&Learning. All rts. reserv.**  
 02903553 844038081  
**Keeping Data Secure**

Simpson, Burney  
 Credit Card Management v18n2 pp: 42-45  
 May 2005

**ISSN: 0896-9329 Journal Code: CCM**

**Document Type:** Periodical; Feature **Language:** English **Record Type:** Fulltext **Length:** 3 Pages

**Special Feature:** Graphs

**Word Count:** 2082

#### **Abstract:**

The string of security breaches and losses this winter of consumer data by several of the country's largest information brokers has politicians of all stripes asking questions and proposing legislation. In the past it usually was the Blue State officials (i.e. Democrats) that sought to rein in the data warehouses that gather and manipulate the mountains of personal information that American consumers generate. But there was U.S. Rep. Joe Barton, chairman of the House Energy and Commerce Committee, suggesting in March a ban on the sale of Social security numbers without the consumer's permission. Perhaps symbolic of the gathering bipartisan approach to the consumer privacy issue, Barton was joined by U.S. Rep. Edward J. Markey, a Massachusetts Democrat, to press for a closer look at the sale of consumer data.

#### **Text:**

Crooks and con men made headlines as they broke through defenses to swipe consumer data. Now Congress wants to crack down on the commercial data houses.

You know you are in trouble when a Texas Republican is after you. The string of security breaches and losses this winter of consumer data by several of the country's largest information brokers has politicians of all stripes asking questions and proposing legislation.

Perhaps symbolic of the gathering bipartisan approach to the consumer privacy issue, Barton was joined by U.S. Rep. Edward J. Markey, a Massachusetts Democrat, to press for a closer look at the sale of consumer data.

Using consumer names as identifiers would put the burden on consumer Betty Jones to ensure that her bank and her phone company and her dentist contacted only Betty Jones with her personal information. And if there is another Betty Jones who is up to no good, the consumer would have to prove she's the innocent one, says Andersen.

It may be that the use of Social Security numbers as an identifier is so pervasive that any ban would be near impossible. But politicians are looking for ways to better regulate how the numbers are safely secured, traded, analyzed and used.

In February, ChoicePoint Inc. went public with the news that it sold records of 145,000 consumers to a ring of crooks in the Los Angeles area. In March, the Alpharetta, Ga.-based firm reported it found that the crooks had attempted to use the information of 750 consumers.

Bank of America Corp. announced in February it had lost tapes with personal data on 1.2 million federal employees that participate in the SmartPay charge card program overseen by the General Services Administration. The Senate and its entire staff were put on notice that their financial information could be affected, according to a legislator's aide who

requested anonymity.

A furious Sen. Patrick Leahy told the Senate Banking, Housing and Urban Affairs Committee that BofA apparently lost the tapes while shipping them by commercial airliner. "We now understand that this type of transport was routine, not only for Bank of America, but for the entire industry," the Vermont Democrat testified.

LexisNexis, a division of Reed Elsevier PLC, reported in March that personal information on 32,000 U.S. residents had been stolen from its database. In April, the company increased the total affected to up to 310,000.

#### Regulatory Options

A LexisNexis spokesperson said the data had come from Seisint, a compiler of consumer information that LexisNexis bought last summer. Merchants DSW Shoe Warehouse and BJ's Wholesale Club also reported in the last year that credit card information had been either lost or stolen from their databases.

Congress held a number of hearings related to the data thefts and losses, and several proposals have come forward that observers believe could earn widespread support.

The possible new regulations affecting the consumer data industry still are being negotiated on Capitol Hill. What appears definite is that companies that use consumers' personal information soon will be seeing tougher restrictions on that data. Further, any firm or person that holds that information will have to be more stringent in controlling outsiders' access to the data.

The collection industry has been vocal on potential legislation because it relies on consumer data to track debtors. One fear is that Congress will overreact and attempt to completely end access to swaths of consumer data.

"Every constituent is interested in privacy. So we hear of these violations. Congress's answer is to regulate," says Stuart R. Blatt, an attorney with collections law firm Margolis, Pritzker, Epstein & Blatt RA. of Towson, Md. "We must get there before (a bill is) passed. We need to form coalitions to educate Congress, and we need a coordinated argument."

Last year, Blatt helped form the Joint Association Summit to find common ground among major collection-industry groups and to present a uniform view to legislators.

Business should have input in defining a data warehouse, says ACA's Andersen, noting that the gathering and storing of consumer information is a basic business fact. "Any commercial enterprise has personal financial data, from the YMCA to Walgreens," she says. Meanwhile, legislators also are listening to privacy advocates such as Evan Hendricks, editor and publisher of the Privacy Times newsletter and author of the book "Credit Scores & Credit Reports." Hendricks told the Senate Banking Committee that consumers should be able to review and correct their personal information held by the consumer-data companies and have a say in how it is used.

For business interests, the silver lining in this dark cloud of proposed legislation is the possible creation of federal standards in the treatment of this information, instead of a mix of state laws.

ChoicePoint's Chairman and Chief Executive Derek Smith spoke for much of the data gatherers when he told a Senate committee his firm would prefer such national preemption. Consumer advocates are wary, however, because of fears that Congress will water down some tough individual state standards.

California has taken the lead in enacting legislation addressing identity theft, possibly because more consumers there are victims of the crime. A California rule requiring data houses to inform affected consumers if their information is breached has been credited with publicizing the loss of data by ChoicePoint.

A survey by Financial Insights found that 13.3% of consumers in the West claimed to be ID-theft victims, nearly double that of the Midwest and South. And 17% of consumers in the West said they were very worried about ID theft, higher than anywhere else in the country. Financial Insights found that 8.4% of consumers nationwide, or nearly 20 million adults, say they have been a victim of identity theft.

#### Enforcement Debate

The Consumer Banking Survey 2005 from the Framingham, Mass.-based Financial Insights involved phone surveys of 1,000 consumers ages 18 and older in January, before the spate of data-loss and theft incidents received widespread public attention.

Political observers also are watching whether the Federal Trade Commission will become the regulator and enforcer of the proposed rules. Members of the Banking Committee clearly were frustrated by the lack of an overarching agency that policed the data-information industry.

California has implemented several privacy-related measures that some officials would like to modify and apply to the national stage. California Democrat Sen. Dianne Feinstein introduced three proposals, one devoted to broad privacy rules and two related to breaches of information.

Feinstein's Privacy Act of 2005 would set national standards on the use and sale of such information as Social Security numbers, driver's license records, and medical and financial data. Companies would have to let consumers "opt in" before their personal information is shared with a third party. And consumers also would have the right to "opt out" if a firm wanted to share such basic contact information as their name and address.

The Privacy Act would make the FTC the regulator of the sale and use of most consumer information, though state attorneys general would enforce criminal use of driver's license information.

The ACA is opposed to putting the oversight of consumer data under the control of one federal agency, says Andersen. "No one agency oversees all the firms that store consumer information," she says. "The FTC does not regulate banks. The Federal Deposit Insurance Corp. and the Office of the Comptroller of the Currency do." It would be better to expand the authority of these regulators to include oversight of consumer data in their areas, says Andersen.

The question of oversight may have been further confused by an announcement in March by four federal banking regulators of new rules on the treatment of identity theft. The FDIC, the Federal Reserve, the OCC and the Office of Thrift Supervision released interagency guidance for financial

institutions, requiring them to implement a response program to security breaches of customer information.

#### Public Disclosure

An institution immediately must inform customers if there has been unauthorized access to their information that could result in harm or inconvenience, according to the guidance. The institutions also must inform their primary federal regulator if a breach of customer information occurs.

The guidance lists the sensitive information as the customer's name, address and phone number combined with Social security number, driver's license number, credit card data or other personal identification numbers. Customer notification can be delayed by the appropriate lawenforcement agency if an investigation is continuing.

Feinstein also has introduced a breach-notification proposal that would require entities that own or license electronic data containing personal information to notify any U.S. resident whose personal information is acquired by an unauthorized person. These data-information houses may delay informing affected consumers pending a police investigation.

#### West Leads in Identity Theft (by % of consumers)

Feinstein's third proposal prohibits the display, sale or purchase of Social Security numbers without consent of the consumer, except in certain circumstances.

Rep. E. Clay Shaw Jr., a Florida Republican, reportedly plans to reintroduce a bill designed to control use of Social security numbers. Shaw introduced a similar proposal several years ago that made it through the powerful House Ways and Means Committee. The bill ran out of time because of congressional adjournment, but the timing could be right this year. Democrat Markey, leader of the Privacy Caucus on Capital Hill, has introduced a likeminded proposal.

#### Executive Liability

Markey teamed with Sen. Bill Nelson, a Florida Democrat, to introduce a measure designed to regulate consumerdata companies. Markey would make the FTC the regulator of the firms, require them to toughen their security measures and allow consumers to access their own data held by the firms.

New Jersey Democrat Sen. Jon Corzine was disseminating in March a draft proposal that would address the consumer data issue much like Gramm-Leach-Bliley addressed financial accountability. According to Corzine's spokesperson, companies would "provide a chief compliance officer or executive officer to personally attest that safeguards are in place that guard against theft or loss of this sensitive (consumer) information." Corzine planned to introduce the measure in April.

#### Passage A Lock?

It is too early to tell the likelihood of any of these proposals becoming law. A veteran lobbyist speaking anonymously notes that Barton and other Republicans are intensely interested in these issues, and Republicans control both the Senate and the House. That puts a near lock on passage of a bill setting national standards on the security of consumer data and tougher penalties for security breaches, the lobbyist believes.

The barrage of news on data theft appears to have touched a nerve in consumers long concerned about the security of their personal information.

It looks inevitable that voters putting pressure on Congress will bring new controls on the consumer data industry.

"I don't want to be in the business of proving I'm not the person they are seeking."

**THIS IS THE FULL-TEXT.**

Copyright Thomson Media May 2005

**Geographic Names:** United States; US

**Descriptors:** Federal legislation; Right of privacy; **Personal information** ; Consumer protection; Financial services; Identity theft; Disclosure

**Classification Codes:** 9190 (CN=United States); 4320 (CN=Legislation); 1200 (CN=Social policy); 8120 (CN=Retail banking)

**Print Media ID:** 12410

ABI/Inform(R) (Dialog® File 15): (c) 2005 ProQuest Info&Learning. All rights reserved.

---

©1997-2005 Dialog, a Thomson business - Version 2.5



**DialogWeb**

Guided Search   new search   favorites   settings   order   cost   login   help

Dynamic Search: ABI/INFORM®, Gale Group Computer Database(TM), Business & Industry(TM), Financial Times Fulltext, Business Wire (Mar 1999-present), The McGraw-Hill Companies Publications Online, Business Wire (1986-Feb 1999), Gale Group New Product Announcements/Plus®

Records for: **"personal information"**   save as alert   save strategy only

Output   Format: **Full Record**   Output as: **Browser**   display/send

Modify   refine search   back to picklist

Records   1   of   1   In full Format

Fulltext available through: **USPTO Full Text Retrieval Options**

1. **6/9/1 (Item 1 from file: 15) DIALOG(R)File 15:ABI/Inform(R) (c) 2005 ProQuest Info&Learning. All rts. reserv.**  
 02903553   844038081  
**Keeping Data Secure**
- Simpson, Burney  
 Credit Card Management v18n2 pp: 42-45  
 May 2005  
**ISSN: 0896-9329 Journal Code: CCM**  
**Document Type: Periodical; Feature Language: English Record Type: Fulltext Length: 3 Pages**  
**Special Feature: Graphs**  
**Word Count: 2082**

**Abstract:**

The string of security breaches and losses this winter of consumer data by several of the country's largest information brokers has politicians of all stripes asking questions and proposing legislation. In the past it usually was the Blue State officials (i.e. Democrats) that sought to rein in the data warehouses that gather and manipulate the mountains of personal information that American consumers generate. But there was U.S. Rep. Joe Barton, chairman of the House Energy and Commerce Committee, suggesting in March a ban on the sale of Social security numbers without the consumer's permission. Perhaps symbolic of the gathering bipartisan approach to the consumer privacy issue, Barton was joined by U.S. Rep. Edward J. Markey, a Massachusetts Democrat, to press for a closer look at the sale of consumer data.

**Text:**

Crooks and con men made headlines as they broke through defenses to swipe consumer data. Now Congress wants to crack down on the commercial data houses.

You know you are in trouble when a Texas Republican is after you. The string of security breaches and losses this winter of consumer data by several of the country's largest information brokers has politicians of all stripes asking questions and proposing legislation.

In the past it usually was the Blue State officials (i.e. Democrats) that sought to rein in the data warehouses that gather and manipulate the mountains of personal information that American consumers generate. But there was U.S. Rep. Joe Barton (RTexas), chairman of the House Energy and Commerce Committee, suggesting in March a ban on the sale of Social security numbers without the consumer's **permission** .

Perhaps symbolic of the gathering bipartisan approach to the consumer privacy issue, Barton was joined by U.S. Rep. Edward J. Markey, a Massachusetts Democrat, to press for a closer look at the sale of consumer data.

A ban on the use of Social security numbers as an identifier would mean a complete revamping of the consumer information databases that issuers, collectors and their vendors use to work with their customers. Moreover, business may be forced to return to using consumer names as an identifier, leading to huge expenses and brainnumbing confusion, says Rozanne M. Andersen, senior vice president of ACA International, the Edina, Minn.-based trade association for collections agencies.

Using consumer names as identifiers would put the burden on consumer Betty Jones to ensure that her bank and her phone company and her dentist contacted only Betty Jones with her personal information. And if there is another Betty Jones who is up to no good, the consumer would have to prove she's the innocent one, says Andersen.

"I don't want to be in the business of proving I'm not the person they are seeking," she says. "That is almost legislative ID theft."

It may be that the use of Social Security numbers as an identifier is so pervasive that any ban would be near impossible. But politicians are looking for ways to better regulate how the numbers are safely secured, traded, analyzed and used.

Capital Hill's focus followed embarrassing reports of theft or loss of consumer data, including information on the legislators and their staffs. In April, retailer Polo Ralph Lauren reported its point-of-sale software was improperly storing data from the GM MasterCard issued by HSBC-Americas. Nearly 200,000 cardholders may have been affected. The retailer announced it first learned of the problem last November, and early indications were that no security breach had occurred.

In February, ChoicePoint Inc. went public with the news that it sold records of 145,000 consumers to a ring of crooks in the Los Angeles area. In March, the Alpharetta, Ga.-based firm reported it found that the crooks had attempted to use the information of 750 consumers.

ChoicePoint gathers consumer data from a mix of public records, bundles it all together and markets it to financial institutions, collectors, employers, landlords and others. In this case the scamsters posed as legitimate businesses seeking the information for marketing purposes. Following the revelations, ChoicePoint announced it would stop selling the data except to government agencies and law-enforcement officials.

Bank of America Corp. announced in February it had lost tapes with personal data on 1.2 million federal employees that participate in the SmartPay charge card program overseen by the General Services Administration. The Senate and its entire staff were put on notice that their financial information could be affected, according to a legislator's aide who

requested anonymity.

A furious Sen. Patrick Leahy told the Senate Banking, Housing and Urban Affairs Committee that BofA apparently lost the tapes while shipping them by commercial airliner. "We now understand that this type of transport was routine, not only for Bank of America, but for the entire industry," the Vermont Democrat testified.

LexisNexis, a division of Reed Elsevier PLC, reported in March that personal information on 32,000 U.S. residents had been stolen from its database. In April, the company increased the total affected to up to 310,000.

#### Regulatory Options

A LexisNexis spokesperson said the data had come from Seisint, a compiler of consumer information that LexisNexis bought last summer. Merchants DSW Shoe Warehouse and BJ's Wholesale Club also reported in the last year that credit card information had been either lost or stolen from their databases.

Congress held a number of hearings related to the data thefts and losses, and several proposals have come forward that observers believe could earn widespread support.

The possible new regulations affecting the consumer data industry still are being negotiated on Capitol Hill. What appears definite is that companies that use consumers' personal information soon will be seeing tougher restrictions on that data. Further, any firm or person that holds that information will have to be more stringent in controlling outsiders' access to the data.

The collection industry has been vocal on potential legislation because it relies on consumer data to track debtors. One fear is that Congress will overreact and attempt to completely end access to swaths of consumer data.

"Every constituent is interested in privacy. So we hear of these violations. Congress's answer is to regulate," says Stuart R. Blatt, an attorney with collections law firm Margolis, Pritzker, Epstein & Blatt RA. of Towson, Md. "We must get there before (a bill is) passed. We need to form coalitions to educate Congress, and we need a coordinated argument."

Last year, Blatt helped form the Joint Association Summit to find common ground among major collection-industry groups and to present a uniform view to legislators.

Business should have input in defining a data warehouse, says ACA's Andersen, noting that the gathering and storing of consumer information is a basic business fact. "Any commercial enterprise has personal financial data, from the YMCA to Walgreens," she says. Meanwhile, legislators also are listening to privacy advocates such as Evan Hendricks, editor and publisher of the Privacy Times newsletter and author of the book "Credit Scores & Credit Reports." Hendricks told the Senate Banking Committee that consumers should be able to review and correct their personal information held by the consumer-data companies and have a say in how it is used.

For business interests, the silver lining in this dark cloud of proposed legislation is the possible creation of federal standards in the treatment of this information, instead of a mix of state laws.

ChoicePoint's Chairman and Chief Executive Derek Smith spoke for much of the data gatherers when he told a Senate committee his firm would prefer such national preemption. Consumer advocates are wary, however, because of fears that Congress will water down some tough individual state standards.

California has taken the lead in enacting legislation addressing identity theft, possibly because more consumers there are victims of the crime. A California rule requiring data houses to inform affected consumers if their information is breached has been credited with publicizing the loss of data by ChoicePoint.

A survey by Financial Insights found that 13.3% of consumers in the West claimed to be ID-theft victims, nearly double that of the Midwest and South. And 17% of consumers in the West said they were very worried about ID theft, higher than anywhere else in the country. Financial Insights found that 8.4% of consumers nationwide, or nearly 20 million adults, say they have been a victim of identity theft.

#### Enforcement Debate

The Consumer Banking Survey 2005 from the Framingham, Mass.-based Financial Insights involved phone surveys of 1,000 consumers ages 18 and older in January, before the spate of data-loss and theft incidents received widespread public attention.

Political observers also are watching whether the Federal Trade Commission will become the regulator and enforcer of the proposed rules. Members of the Banking Committee clearly were frustrated by the lack of an overarching agency that policed the data-information industry.

California has implemented several privacy-related measures that some officials would like to modify and apply to the national stage. California Democrat Sen. Dianne Feinstein introduced three proposals, one devoted to broad privacy rules and two related to breaches of information.

Feinstein's Privacy Act of 2005 would set national standards on the use and sale of such information as Social Security numbers, driver's license records, and medical and financial data. Companies would have to let consumers "opt in" before their personal information is shared with a third party. And consumers also would have the right to "opt out" if a firm wanted to share such basic contact information as their name and address.

The Privacy Act would make the FTC the regulator of the sale and use of most consumer information, though state attorneys general would enforce criminal use of driver's license information.

The ACA is opposed to putting the oversight of consumer data under the control of one federal agency, says Andersen. "No one agency oversees all the firms that store consumer information," she says. "The FTC does not regulate banks. The Federal Deposit Insurance Corp. and the Office of the Comptroller of the Currency do." It would be better to expand the authority of these regulators to include oversight of consumer data in their areas, says Andersen.

The question of oversight may have been further confused by an announcement in March by four federal banking regulators of new rules on the treatment of identity theft. The FDIC, the Federal Reserve, the OCC and the Office of Thrift Supervision released interagency guidance for financial

institutions, requiring them to implement a response program to security breaches of customer information.

#### Public Disclosure

An institution immediately must inform customers if there has been unauthorized access to their information that could result in harm or inconvenience, according to the guidance. The institutions also must inform their primary federal regulator if a breach of customer information occurs.

The guidance lists the sensitive information as the customer's name, address and phone number combined with Social security number, driver's license number, credit card data or other personal identification numbers. Customer notification can be delayed by the appropriate lawenforcement agency if an investigation is continuing.

Feinstein also has introduced a breach-notification proposal that would require entities that own or license electronic data containing personal information to notify any U.S. resident whose personal information is acquired by an unauthorized person. These data-information houses may delay informing affected consumers pending a police investigation.

#### West Leads in Identity Theft (by % of consumers)

Feinstein's third proposal prohibits the display, sale or purchase of Social Security numbers without consent of the consumer, except in certain circumstances.

Rep. E. Clay Shaw Jr., a Florida Republican, reportedly plans to reintroduce a bill designed to control use of Social security numbers. Shaw introduced a similar proposal several years ago that made it through the powerful House Ways and Means Committee. The bill ran out of time because of congressional adjournment, but the timing could be right this year. Democrat Markey, leader of the Privacy Caucus on Capital Hill, has introduced a likeminded proposal.

#### Executive Liability

Markey teamed with Sen. Bill Nelson, a Florida Democrat, to introduce a measure designed to regulate consumerdata companies. Markey would make the FTC the regulator of the firms, require them to toughen their security measures and allow consumers to access their own data held by the firms.

New Jersey Democrat Sen. Jon Corzine was disseminating in March a draft proposal that would address the consumer data issue much like Gramm-Leach-Bliley addressed financial accountability. According to Corzine's spokesperson, companies would "provide a chief compliance officer or executive officer to personally attest that safeguards are in place that guard against theft or loss of this sensitive (consumer) information." Corzine planned to introduce the measure in April.

#### Passage A Lock?

It is too early to tell the likelihood of any of these proposals becoming law. A veteran lobbyist speaking anonymously notes that Barton and other Republicans are intensely interested in these issues, and Republicans control both the Senate and the House. That puts a near lock on passage of a bill setting national standards on the security of consumer data and tougher penalties for security breaches, the lobbyist believes.

The barrage of news on data theft appears to have touched a nerve in consumers long concerned about the security of their personal information.

It looks inevitable that voters putting pressure on Congress will bring new controls on the consumer data industry.

"I don't want to be in the business of proving I'm not the person they are seeking."

**THIS IS THE FULL-TEXT.**

Copyright Thomson Media May 2005

**Geographic Names:** United States; US

**Descriptors:** Federal legislation; Right of privacy; **Personal information** ; Consumer protection; Financial services; Identity theft; Disclosure

**Classification Codes:** 9190 (CN=United States); 4320 (CN=Legislation); 1200 (CN=Social policy); 8120 (CN=Retail banking)

**Print Media ID:** 12410

---

ABI/Inform(R) (Dialog® File 15): (c) 2005 ProQuest Info&Learning. All rights reserved.

©1997-2005 Dialog, a Thomson business - Version 2.5